Access Control & Biometrics

Nataliya B. Sukhai
6675 Williamson Drive
Atlanta, Georgia 30328
+1 404-943-1019
nbsukhai@att.net

ABSTRACT

This paper introduces readers to the world of information technology and data security as a part of it. It talks about access control, its components, and levels and types of access control. The paper recognizes the importance of identifying and authenticating any given user in the business areas. Therefore, it gives full attention to biometrics as one of the access control technology and discusses variety and performance of other known techniques; points out the advantages and disadvantages of using them. The paper also presents some real life examples of companies, implementing biometric solutions in their businesses.

CATEGORIES AND SUBJECT DESCRIPTORS

D.4. 6 [**Operating Systems**]: Security and Protection- *access controls, authentication.*

GENERAL TERMS

Security

KEYWORDS

Access Control, Biometrics.

INTRODUCTION

We live in the era of digital kingdoms and computer slaves, who make human life much easier, but not necessary more secure. Just think how simple it was back in the Stone Age when probably the only valuable data was on a gigantic stone, where to steal or modify such a thing would require a tremendous human strength. Even just few decades ago to commit a crime one had to think of a way to do it, being visible, touchable, and recognizable. In other words one had to be physically present at the scene of a crime. Today, it is easier than ever to commit a felony. While some individuals are still trying to rob banks and sell drugs personally, many discovered a more comfortable way. In the privacy of their own home they compensate sleepless nights and absence of social life by mastering their computer skills, aimed to get into the unreachable. It starts as a joke or a new challenge, but often grows into an illegal activity. Why just search the Internet, when there are ways to modify it and force to play your own games? Who likes to work to make money when it is possible to change a payroll and get a bonus? Invisible criminals succeed and it is getting harder and harder to catch and prosecute those who dare to intrude the security areas.

InfoSecCD Conference'04, October 8, 2004, Kennesaw, GA, USA.

1. OVERVIEW OF ACCESS CONTROL

Fast growing, constantly changing world of Information Technology demands fast responding and reliable security devices. Every day our world converts more business data into an electronic format, and we are obligated to protect information from those lacking social life individuals, who cannot sleep well at night or from those unethical persons who just want to explore the possibilities.

Confidential data, the heart of any organization, is vulnerable to attacks, with attacks coming from both outside and inside of a company. Assuming that outside hackers are restricted (at least until the new hacking tool comes out) by firewalls and encryptions, then we have to wary about the insiders or strangers who can get inside.

Keeping data secure means that we need to make sure that any access to data is supervised. One of the most important parts of any secure environment is the employees themselves. They represent the "Human firewall" inside the organization; they must be trained to behave securely and monitor the surroundings. The Information System Security Association (ISSA) designed a "human firewall" web site, built to educate people, to provide with the survey to evaluate their security level and in general to make individuals aware of possible threats. Dave Cullinane, ISSA president said: "We find that people are generally aware of the danger out there, but not aware of what they should do to keep their systems secure" (Kawamoto D., 2004).

Now that employees are aware of the dangers, alert to any suspicious activities, and outsiders are kept securely at a distance, does it mean the precious data is safe? Not really. Now we need to worry that only authorized people can access data and hope that they do not intend to cause any harm. We need to make sure access is easy but properly secured for physical access to a building to retrieve necessary information in the work place.

1.1. Components of Access Control

Proper identification, authentication, authorization, accountability are the important components of an access control, a process that relays on its components to enforce security. We start with identifying users, and then we verify the identity by authenticating them, making sure they are who they claim they are. If we are successful in these steps, authorization component checks what levels of information users are allowed to access, what tasks they can execute and then permits a connection to the system. Another important role is played by the accountability part of an access control. It monitors and records all activities performed by an authenticated user so if necessary, a user can be hold accountable for the actions accomplished.

The main underlying idea of an access control process is to protect the confidentiality, integrity and availability of data. It means that we want data to be protected from unauthorized viewing; we want data at any retrieving time to be in the same state as it is expected to be; we want data to be highly secure but easily available, finding a balance between security and accessibility.

We can be proactive in dealing with access control, making sure all financially possible precautions are done and therefore reducing a risk of a threat. Proactive control can be achieved through new employees' background checking when hiring them, through continuously security awareness training of the personnel, through an implementation of a company's policies. Separation of duties, split knowledge and data classification are also good ways of access control to make sure people are exposed only to the information they are authorized to.

Physical layers of protection can be enforced through fences, guard dogs and locks outside an organization. At the point of entry it is a good practice to have alarms for after-hours control, and ID badges, Icard-key, tokens and biometrics devices to control, record and monitor daily flow of employees. Passwords and now biometrics protect the actual access to data.

1.2. Types of Access Control

The main component of an access control process is authentication of an individual. There are three major types of authorization. An authentication can be performed using some memorized knowledge, like a pin, password, password phrase, and mother's maiden name -something you know. It can be done using some touchable and visible documents like passport, drivers license, ID card, key, ATM card -something you have. It can also be done through the process of comparing what a person is, like ones fingerprints, signature, voice, iris, retina, DNA, hand geometry-something you are (Whitman M., 2004).

1.3. Multi-factors of Access Control

To achieve the highest level of security, interested companies use a multiple factor authentication, combining the types of it. In a two-factor of authentication a user may be asked to provide an ATM card and a pin; username and password; a credit card, a signature. In three-factor authentication it may be username, password and SecurID token; username, password and fingerprint (Rothke, 2004). According to Whitman M. and Mattord H. book "Management of Information Security", strong authentication includes "…at minimum two different mechanisms (usually something you have and something you know)…called two-factor authentication, because two separate identification mechanisms are used." Banking card and a personal identification number is provided as an example. It's recommended to use something other than what we know to accomplish strong authentication (Whitman M. and Mattord H, 2004).

2. BIOMETRICS

The last type of authentication, the one relies on measurable physical characteristics that can be automatically checked, and is becoming more popular and demanded. It is called biometrics. Every individual is unique, while the overall human structure is the same; this approach puts biometrics in a great demand in the constantly updating field of security. Though the approach is still in its infancy, many people believe that biometrics will play a critical role in future computers, and especially in electronic commerce.

It seems like every part of a human body was tested to determine if it is produce a unique pattern: face and ear shapes, voice and odor, retina and iris, fingerprints, DNA, gait and veins of a hand. Obviously for convenience reasons, only normally visible parts of a body were implemented; probably users wouldn't want to take the shoes off to measure a toes pattern or the pressure applied while walking. May be someday we will be authenticating people by a heart beat or a spit out, it all depends on the progress we are making in the field, the demand of different identifiers and hackers success in reproducing someone's characteristics.

2.1. Elements of Biometrics

For now several identifiers are accepted and used in the real world. They are: face recognition, retina scan, iris, voice recognition, vascular patterns, hand geometry, fingerprints, keystrokes and signature recognition.

Digital cameras are used not only to take pictures, but also to capture, analyze and compare to database records the overall facial structure, including distances between eyes, nose, mouth, and jaw edges. A user usually stand within two feet from the camera and most of the time is required to perform some human facial movement, like smile or blink to prevent a system from positively identifying a mold or fake face. The decision is typically made in less than 5 seconds.

Human eyes are very unique and hard to fake. Two methods are used based on that. Retinal scanning analyzes the layer of blood vessels at the back of the eye. Scanning uses a low-intensity light source and an optical coupler. A person is required to keep his head still, look closely in the device and focus on a green light while scanning is performed. The whole process takes 10-15 seconds. Since there is no known way to reproduce a retina, and one from a dead person would weaken too soon, no additional precautions are taken to prevent faking a living human. Another method of eye recognition is iris- analysis of more than 200 points in the colored tissue surrounding the pupil. In this case user can be either close to the video camera or 2 feet away, depending on the device. Iris recognition does not use infrared light beams, so it

is safer to an eye. The identification is done in less than 5 seconds and may use light shone to watch for pupil dilation to prevent users from fooling the system. Both methods do not require users to remove glasses.

Voice recognition is a process of validation a pass phrase thought the microphone. Another under 5 second authentication requires a user to reproduce low and high sound frequencies.

Face or hand vein thickness and their locations are considered being unique enough to identify a person. An infrared scan from a curved reader device performs a vascular scanning process and then compares it to the database records to find a match.

A user places a hand on the metal plate with guides on it to take more than 90 measurements of the length, width, thickness and surface of the hand and a number of fingers with hand geometry scan. It is a simple, fast and accurate procedure, but unable to tell the difference between a living and a fake or a dead hand, if pressure is properly applied. Unfortunately, human hand geometry is not unique, although if a way will be developed to combine hand geometry with any other method, the authentication process can be successfully used.

One of the oldest ways to check a person's identity is fingerprinting. With fingerprinting a user gently places fingers against a small reader device. Characteristics such as whorls, arches, and loops are recorded along with the patterns of ridges, furrows, and minutiae. Depending on the security level in the organization, some of them require six or seven identical points, where law enforcement agencies prefer twelve. Most of the time, no actual image is created, only some data that can be used for comparison. This method was design to calm public reaction on possibility of fingerprints images being stolen. The system fake prevention techniques include measurements of blood flow or correctness of arrayed ridges at the edge of the fingers.

Person's ability to write something either by hand or using a keyboard is unique too. When typing on the keyboard, a system records the timing of a keystroke process and then compares the password or passes phrase itself, as well as the recorded timing. Signature recognition works on the record device or on the piece of paper over a sensor tablet and also compares the given and stored result. Both methods are quick, take less than 5 seconds and seem easy to fake.

No longer is used, but very interesting the bertillonage method was created in 1890' by Alphonse Bertillon, a Paris police clerk, who was also an anthropologist. He based this method on a claim that bones do not grow after age 20, so measurements of anyone after that age should remain the same. As a result, 20-60 minutes measuring procedure was done to identify criminals. The records of length, height, breath of heads, fingers, arms, and legs… were done by hand and filed. It was relatively fast and effective method for that time, until two different people had the same measurements. Paris police switched to fingerprinting, which soon became widely spread and bertillonage was forgotten (Networks and Telecommunications Research Group, 2004).

3. ADVANTAGES AND DISADVANTAGES OF BIOMETRICS

As with any other technology, biometrics has its own advantages and disadvantages. The best reason why biometrics is getting more popular and widely implemented is a convenience of having authenticating mechanisms with a user. We can't forget parts of our body at home, and we can't lend it. We don't need to memorize fingerprints and then change it every 3 months as with passwords. Biometrics can last virtually forever, until something is amputated or damaged.

On the opposite side, there is a factor of users accepting or not accepting a particular biometric technique. Some people are still hesitant to be authenticated using fingerprints, since it was associated for a long time with criminals and prisons. However, most people accept voice recognition. Retina and iris recognitions trouble some people due to the exposure to the light, which they consider to be harmful for the eyes. Good news is that improvements in eye recognition allow users to be scanned from up to12 inches away from the camera.

Most biometric technologies are patented, which means it is very expensive to companies to license the use and implementation of any type of biometrics. Fortunately, some patents will expire within 3 years, allowing more businesses to implement biometrics at a lower cost, keeping a concern to get a profitable return on technical investment (Bowcott, 2004).

According to Networks and Telecommunications Research Group finding of July 2004, the cost of biometric authentication is still high. In addition to purchasing hardware and software, the integration into the current network needs to be considered. Simplistic networks work the best with biometrics devices, where most companies use more complicated network configuration. The research group presents an "all or nothing technology", meaning that "…there is no point in having biometric authentication at every desktop on your network if someone using a laptop can remotely login in with no biometric authentication as this would completely undermine the system" (Networks and Telecommunications Research Group, 2004).

Companies agree that the most reliable biometrics are fingerprints and iris scans, but are also concern with the accuracy of devices. It is possible to fool some of them, known cases include recreating one's hand prints out of gelatin or children's modeling material. Facial recognition can be difficult due to people preferences of facial hair, bloating of pregnant women or just long time travelers. Voice recognition can suffer because of users' sickness as a sore throat or lost of voice; and high quality recording would attempt to reproduce ones voice.

Another big issue in biometric implementation is software support for the biometric hardware devices. This problem is rapidly disappearing though. A consortium known as the BioAPI group aims to develop a widely available and widely accepted API (Application Programming Interface) that will serve for various biometric technologies. This API is intended to be Operating system and Biometric Data independent. Already vendors are announcing products that are compliant to the BioAPI standards. Gateway is advertising laptops with a build-in biometrics. Microsoft can't stay away from such an important issue too; in the spring of 2000 Microsoft announced that upcoming versions of Windows would have biometrics technology integrated into them (Networks and Telecommunications Research Group, 2004).

4. IMPLEMENTATION OF BIOMETRICS

Despite all disadvantages some companies implement biometrics in variety of areas, like network access control, staff time and attendance, tracking, authorization of financial transactions,

Government benefits distribution, verification of identities at point of sale, usage in conjunction with ATM, control of physical access to office buildings or homes, voting and document verification such as passports, visas & immigration.

Websites and newspapers, journals and magazines provide examples of companies implementing biometrics. Thus, Palace Casino in West Edmonton Mall had used a face recognition system since 2001, mainly to identify problem visitors, cheaters and keep them out. The casino is currently installing handprint time clocks for the about 360 staff personnel to eliminate the possibility of one employee clocking in for another one. The airport iris-scanning system, called CANPASS-Air, will be installed at Edmonton International airport in the fall 2004 as part of the joint Canada-U.S. "smart border" program. Passengers who frequently cross the border can pay $50 a year to join the program and will be allowed to bypass custom and immigration lines, using iris scanning technique (Finlayson, 2004).

5. CONCLUSION

So, why do we need biometrics? The main use in networking security will be the replacement of current system of passwords. It is not a secret that humans forget their passwords, especially if they need to use several different ones and change them every so often. They forget passwords and end up being locked out of the system. Then they call either call a help desk or a system administrator to regain an access. If it is a large organization then a lot of time is wasted to let users in and a company doesn't increase its profitability. Another problem with passwords exists when users write passwords down and post it somewhere nears a computer. This breaches policy and eliminates the reason for security.

As technology improves and costs come down we shall see an increase in biometric security, especially since Microsoft is coming up with the built-in biometrics and we all greatly depend on Microsoft products. What is most likely to happen is the widely accepted combination of biometric authentication (what we are) with some kind of IDcards or tokens (what we have), or may be the era of even more complicated systems of verifying an identity.

It is a bit scary, the farther we get into the 21-century, the more we depend on the machines to keep our personal data and less we are the owners of our data. Who owns our personal information? Databases and organizations they belong to, like medical and law agencies, educational and retail businesses. They still do a good job trying to protect it and using modern techniques, including biometrics. We just need to learn to trust them.

Coming back to our sleepless intruders or adventurous employees; Biometric control access to sensitive data via network connections, port of entry or system login will definitely make their job harder, if not impossible. Unless bad guys (as seen in modern movies about secret laboratories) kill the right person in front of ATM machine in the public place, pop out his eye and stick it into the eye recognition device to gain access to the account, we don't have a reason to worry about our own safety.

6. REFERENCES

[1] Bowcott O. June 18, 2004. Ear, iris, odor: search for the perfect system. *The Guardian*. Retrieved June 26, 2004 from http://www.guardian.co.uk/humanrights /story /0,7369,1241847,00.html

[2] Finlayson D. June 18, 2004. Biometric ID business takes off. Endless new applications found for fingerprint, retina, and voice recognition. *The Edmonton Journal*. Retrieve June 26,2004 from http://www.canada.com/edmonton /edmontonjournal/ news/business /story.html?id=bef0fee8-b925-4102-b1ee-4ea1391e5223&page=3

[3] Individual biometrics. *Networks and Telecommunications Research Group*. Retrieved June 26, 2004 from http://ctl.ncsc.dni.us/biomet%20web/BMIris.html.

[4] Intranet Journal Staff. November 2003. Access Control 101. Retrieved June26, 2004 http://www.intranetjournal.com/articles/200311/ij_11_10_03a.html

[5] Kawamoto D. Human Firewall gets new owner. June 2004. *CNET News.* Retrieved June26, 2004 from http://news.com.com/2100-7349-5247947.html

[6] Longworth D. Specifying Your Access Control System. *Facility Management*. Retrieved June26, 2004 from http://www.facilitymanagement.com/articles/artacc2.html

[7] Moore M. What is Biometrics? *Darwin Magazine*. Retrieved June 26, 2004 from http://www.darwinmag.com/learn/curve/column.html?ArticleID=160

[8] Rothke B. Access Control Systems & Methodology. *New York Metro eSecurity Solutions Group.* Retrieved June26, 2004 from http://www.cccure.org/ Documents/Ben_Rothke/ Access%20Control.ppt

[9] Schneier B. *Digital Security in a Networked World*. New York: John Wiley and Sons, 2000.

[10] What is Biometrics and why use it in for Network. *Networks and Telecommunications Research Group*. Retrieved June 26, 2004 from http://ntrg.cs.tcd.ie/ undergrad/4ba2.02/ biometrics/whatis.html

[11] Whitman, Michael E. and Mattord, Herbert J. *Management of Information Security.* Boston, Massachusetts: Thomson Course Technology, 2004, 363-375